ガロア体

情報数理学特別講義I 第3回

2025-11-04

ガロア体

計算機やデジタル回路上で，データを誤り訂正符号化する際，有限体上の演算が行われる．
有限体は19世紀フランスの数学者エヴァリスト・ガロアの名をとりガロア体とも呼ばれる．
ガロア体の中で，最も基礎的な体は2元体である．

まず体とその基本となる群についての定義を述べた後，誤り訂正符号で多用する2元体$GF(2)$及びその拡大体$GF\left(2^q\right)$について述べる．

群(group)

以下に述べる3つの性質を満たす演算 '$\cdot$' が定義された元の集合 G を群と呼ぶ.

- 演算 '$\cdot$' が結合則を満たす. つまり任意の $a, b, c \in G$ に対して,
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$
- G が単位元 e をもつ. つまり $\forall a \in G$ に対して,
$$a \cdot e = e \cdot a = a.$$
- 任意の $a \in G$ に対して, ひとつの逆元 $a^{-1} \in G$ が存在する. つまり,
$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

もし演算 '$\cdot$' が可換な場合, つまり $\forall a, b \in G, a \cdot b = b \cdot a$,
この群はアーベル群もしくは可換群と呼ばれる.

整数の集合は和の演算(加算)に関してアーベル群となる. この群では 0 が単位元となる.
結合則を満たすことは明らかで, 整数 a の逆元は $-a$ となる.

体(field)

加算 '+' と積の演算(乗算) '$\cdot$' の2つの演算を持ち，下記性質を満たす元の集合 F を体と呼ぶ.

- 体 F の元は，加算 '+'に関して可換群をなす.
  加算 '+'における単位元を体のゼロ元'0'と呼ぶ.
- 体 F の**非ゼロ元**は，乗算 '$\cdot$'に関して可換群をなす.
  乗算 '$\cdot$'における単位元を体の単位元 '1' と呼ぶ.
- 乗算が加算に関して分配則を持つ．つまり任意の $a, b, c \in F$ に対して,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

体を確認しよう

整数5で剰余をとる加算 '+' と乗算 '·' が定義された整数の集合 $F = \{0, 1, 2, 3, 4\}$ は体をなす($GF(5)$). '0' と '1' はそれぞれ体 F のゼロ元と単位元である.

練習問題(10分)：$GF(5)$ が体であることを確認せよ.

どう確認するか？

- 加算に関して可換群をなすことを確認する.
- 乗算に関して非ゼロ元が可換群をなすことを確認する.
- 乗算が加算に対して分配則を満たすことを確認する.

ガロア体（または素体） $GF(p)$

ガロア体 $GF(p)$ とは，素数 p で剰余をとった数の集合で，素体とも呼ばれる.

$$GF(p) = \{0, 1, \ldots, p-1\}$$

$GF(p)$ 上の加算と乗算は，演算後の値を p で割った剰余で計算する.

$$a + b = (a + b) \bmod p$$
$$a \cdot b = (ab) \bmod p$$

先の例では $GF(5)$ が体をなすことを確認しました.
ここでは，$GF(5)$ 上の計算をやってみよう（２分）.
(1) $2 \cdot 3$ (2) $2 \div 2$ (3) $3 \div 2$

- ヒント：割り算は逆元を使って解こう.

4で剰余をとったら $GF(4)$ になるか？

整数4で剰余をとる加算 '+' と乗算 '·' が定義された整数の集合
$F = \{0, 1, 2, 3\}$ は体をなすか？

練習問題(5分)：加算表と乗算表を作って確認してみよう

剰余をとる数が素数じゃない場合は体が構成できない

4で剰余をとった整数の集合では $GF(4)$ が構成できない（2の逆元が存在しない）
しかし，実用的にはガロア体のサイズは2のべき乗 2^q が望ましい.

- 計算機の中は全て2のべき乗で表現されているため.

どのようにして作ればよいか？

2元拡大体 $GF(2^q)$

サイズが 2^q のガロア体 $GF(2^q)$ は $GF(2)$ 上の q 次の既約多項式 $p(x)$ を用いて構成する.

- 複素数体が実数体上の $1+x^2$ の根 i を用いて構成されるのと同じ.

既約多項式とは，その多項式自身もしくは1以外で割ることができない多項式である.

- 2次以上の多項式において，0 を根に持つならば x で，1 を根にもつならば，$1+x$ で割り切れる.
- $1+x^2$ は実数体上の既約多項式.

クイズ：

1. $1+x^2$ は $GF(2)$ 上の既約多項式か？
2. $1+x+x^2$ は $GF(2)$ 上の既約多項式か？

$GF(2^2)$ を多項式で定義する.

$GF(2^2)$, サイズが4のガロア体 $GF(4)$, を多項式で定義する.
つまり, $GF(4) = \{0, 1, x, 1+x\}$. ＊剰余類 $GF(2)[x]/(p(x))$ である.
いま, $GF(4)$ 上の元 $a(x) = a_0 + a_1 x$ と $b(x) = b_0 + b_1 x$ があるとする.
ただし, $a_0, a_1, b_0, b_1 \in GF(2)$.
加算は $a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x$ で, $GF(4)$ の元に戻る.
加算は可換群の性質を満たす.

$GF(4)$ の乗算

乗算は既約多項式 $p(x) = 1 + x + x^2$ で剰余をとって，集合の元に戻るようにする.

$$
\begin{aligned}
a(x) \cdot b(x) &= (a_0 + a_1 x) \cdot (b_0 + b_1 x) \\
&= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + a_1 b_1 x^2 \\
cx^2 \text{ を } 1 + x + x^2 \text{ で割った余りは } c + cx \text{ なので，剰余は} \\
&= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + a_1 b_1 + a_1 b_1 x \\
&= (a_0 b_0 + a_1 b_1) + (a_0 b_1 + a_1 b_0 + a_1 b_1) x
\end{aligned}
$$

このように乗算を定義することで，乗算も可換群の性質を満たすことができる.

練習問題: $GF(4)$ の乗算表を作成せよ（５分）.

以下の乗算表を埋めてください.
ただし乗算は既約多項式 $p(x) = 1 + x + x^2$ で剰余をとった式とする.

$$\begin{aligned} a(x) \cdot b(x) &= (a_0 + a_1 x) \cdot (b_0 + b_1 x) \\ &= (a_0 b_0 + a_1 b_1) + (a_0 b_1 + a_1 b_0 + a_1 b_1) x \end{aligned}$$

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0			
x	0			
$1+x$	0			

$GF(4)$ の演算表

Table 1: Addition

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

Table 2: Multiplication

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

4で剰余をとった整数の集合では $GF(4)$ が構成できなかったが，このように既約多項式の剰余の集合(剰余類 $GF(2)[x]/(p(x))$)では，加算，乗算ともに可換群の性質を満たし，体となる.
素体における素数の役割を，2元拡大体では既約多項式が担っている.
任意の $GF(2^q)$ に対しても，q 次の既約多項式の剰余の集合は体となる.

$f(x) \in GF(2)[x]/(p(x))$ と $\alpha \in GF(2^q)$ の関係

$GF(2)[x]/(p(x))$ の各元は次数 $q-1$ 以下の多項式を代表元として選べば一意に書ける.

- $[x]$ を新しい元 α と呼ぶと，α は $p(x)$ の根として振る舞い $p(\alpha)=0$ が成り立つ．これは $p(x)$ を剰余類に代入すると $[p(x)]=[0]$ になることと同じ意味である.
- 任意の剰余類 $[f(x)]$ は $\sum_{j=0}^{q-1} a_j \alpha^j$ という形に対応し，各係数 a_j は $GF(2)$ の元である.
- 多項式の加算や乗算を $p(x)$ で割った剰余に戻す操作は，α の冪に書き換えて計算する操作と一致する.
  例：$GF(2)[x]/(1+x+x^2)$ では $[x]=\alpha$，$[x^2]=\alpha^2$ であり，$p(\alpha)=1+\alpha+\alpha^2=0$ より $\alpha^2=\alpha+1$ と書ける．これは x^2 を $p(x)$ で割った剰余が $x+1$ になることと同じである.

既約多項式の根

2元拡大体 $GF(2^q)$ を構成するために q 次の既約多項式 $p(x)$ を導入することを述べた.
既約多項式は $p(x)$ は $GF(2)$の元を根に持たないため，新たに変数を導入し，
$p(x)$ の根を α とする．つまり，$p(\alpha) = 0$.
※複素体における複素数 i (電気系だと j) の役割．符号理論では多項式の根に
α, β などのギリシャ文字を使うことが多い.

なお，$p(x)$ の根 α は $GF(2^q)$ の元である．つまり $\alpha \in GF(2^q)$.

原始元と原始多項式

定義：原始元

ガロア体 $GF(2^q)$ の元 a が原始元であるとは，$GF(2^q)$ の全ての非零元が a のべきで表現できることをいう．

- $a^i = 1$ となる 0 より大きな最小の i を**位数**という．
- a の位数が $2^q - 1$ であるとき，a を**原始元**という．

定義：原始多項式

$GF(2^q)$ の元 α が原始元であるとき，α を根に持つ既約多項式を**原始多項式**という．

※ α はガロア体を構成する原始多項式の根（原始元）として使われることが多い．一方 a はガロア体の任意の元として使われることが多い（気がする）．著者の好みに依存．

$GF(2^q)$ 上の元の表現

$GF(2)$ の元は 0と 1しかないため，表現は一意だが，$GF(2^q)$ を元はその表現が複数ある．
ここでは主要な3つの表現（べき表現，多項式表現，ベクトル表現）を説明する．

$GF(2^q)$ 上の元の表現：べき表現

原始元 α のべき α^i で元を表現することをべき表現と呼ぶ．乗算がべき指数の和で計算できるので乗算計算に便利な表現である．なお，ゼロ元は0で表現する．

例： α^i と α^j の乗算

$$\alpha^i \cdot \alpha^j = \alpha^{i+j \bmod (2^q-1)}$$

$GF(2^q)$ 上の元の表現：多項式表現

$p(\alpha)=0$ より $\alpha^q = p(\alpha) + \alpha^q$ となることから，べき指数 $i \geq q$ の元 α^i はべき指数 q 未満の元の線形和で表現できる.

$$\alpha^i = \sum_{j=0}^{q-1} a_j \alpha^j,$$

ただし， $a_j \in GF(2)$.
このように $GF(2^q)$ の元をべき指数 q 未満の元の線形和で表現することを多項式表現と呼ぶ．なお，この多項式表現は先に説明した x^i を $p(x)$ で割った剰余と同じである.
（x が α になっていると思えば良い）.
本講義では，多項式で表現した $GF(2^q)$ の元をしばしば $a(\alpha)$ のように表す.

$GF(2^q)$ 上の元の表現：ベクトル表現

あらかじめ定めた q 個の基底 $e_0, e_1, \ldots, e_{q-1}$，ただし $e_j \in GF(2^q)$，の線形和

$$\alpha^i = \sum_{j=0}^{q-1} a_j e_j,$$

の係数 $a_j \in GF(2)$ を要素に持つ長さ q のベクトル $(a_0, a_1, \ldots, a_{q-1})^{\mathrm{T}}$ を使った元の表現をベクトル表現と呼ぶ．ただし記号 T は転置である．
最もよく用いられる基底は $e_j = \alpha^j, 0 \leq j < q$ としたもので，標準基底と呼ばれる．
標準基底を用いる場合，ベクトル表現は多項式表現の係数を要素にした長さ q のベクトルとなる．

$$
\begin{aligned}
\alpha^i &= (e_0, e_1, \ldots, e_{q-1}) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{q-1} \end{pmatrix} \\
&= (1, \alpha, \ldots, \alpha^{q-1}) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{q-1} \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{q-1} \end{pmatrix} = (a_0, a_1, \ldots, a_{q-1})^{\mathrm{T}}
\end{aligned}
$$

$p(x) = 1 + x + x^3$ で定義された $GF(2^3)$

Power repr.	Polynomial repr.	Vector repr.
0	0	$(0,0,0)^{\mathrm{T}}$
α^0	1	$(1,0,0)^{\mathrm{T}}$
α^1	α	$(0,1,0)^{\mathrm{T}}$
α^2	α^2	$(0,0,1)^{\mathrm{T}}$
α^3	$1+\alpha$	$(1,1,0)^{\mathrm{T}}$
α^4	$\alpha+\alpha^2$	$(0,1,1)^{\mathrm{T}}$
α^5	$1+\alpha+\alpha^2$	$(1,1,1)^{\mathrm{T}}$
α^6	$1+\alpha^2$	$(1,0,1)^{\mathrm{T}}$

加算

$GF(2^q)$ 上の加算は，元をベクトル表現した際の要素毎に $GF(2)$ の加算をすればよい.
いま，$a = (a_0, a_1, \ldots, a_{q-1}) \in GF(2^q), b = (b_0, b_1, \ldots, b_{q-1}) \in GF(2^q)$ とすると,

$$a + b = (a_0 + b_0, a_1 + b_1, \ldots, a_{q-1} + b_{q-1}).$$

と計算する.

乗算

元をべき表現にすると，$GF(2^q)$ 上の乗算は冪指数の和で計算できる.
いま，$\alpha^i \in GF(2^q), \alpha^j \in GF(2^q)$ とすると,

$$\alpha^i \cdot \alpha^j = \alpha^{i+j \bmod (2^q-1)}.$$

で計算できる.

表現によって得意不得意がある.

べき表現では，各元はべきの値，つまり α^i の i で表現する.
→乗算に有利

ベクトル表現では，各元はベクトルの値，つまり $(a_0, a_1, \ldots, a_{q-1})^{\mathrm{T}}$ で表現する.
→加算に有利

ソフトウェアでガロア体の演算を実施する場合には，べき表現とベクトル表現を変換するテーブルを用意することで，各表現の長所を生かすことができる.
一方，ハードウェア（回路）実装の際には，ベクトル表現を用いることが多い.

ベクトル表現のまま乗算したい

加算が要素毎に $GF(2)$ の加算，つまり2入力XORゲートで実現できることから，
$GF(2^q)$ 上の演算を回路へ実装する際，一般的にはベクトル表現を用いる．
そのため，乗算回路はベクトル表現の入力に対してベクトル表現の乗算結果を出力しなければならない．
入力後にベクトル表現をべき表現に変換し，出力前にべき表現をベクトル表現に変換することで，べき表現の乗算を用いることもできるが，ガロア体のサイズが大きくなると変換回路のコストが大きくなるため，通常は多項式表現を使ってベクトル表現のままの乗算回路を実装する．

多項式表現での乗算

いま，$a = (a_0, a_1, \ldots, a_{q-1}) \in GF(2^q), b = (b_0, b_1, \ldots, b_{q-1}) \in GF(2^q)$ とすると，元 a, b はそれぞれ多項式表現により

$$a(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{q-1}\alpha^{q-1}, b(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{q-1}\alpha^{q-1},$$

と表現できる．よって $a \cdot b$ は多項式表現を用いて

$$\begin{aligned} a(\alpha) \cdot b(\alpha) &= a_0 b(\alpha) + a_1 \alpha b(\alpha) + a_2 \alpha^2 b(\alpha) + \cdots + a_{q-1}\alpha^{q-1} b(\alpha), \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)\alpha + (a_0 b_2 + a_1 b_1 + a_2 b_0)\alpha^2 + \cdots + a_{q-1} b_{q-1} \alpha^{2q-2}, \end{aligned}$$

と計算できる．最大次数 $2q-2$ の多項式となっているが，拡大体を構成するための既約多項式 $p(x)$ を用いて冪指数 $i \geq q$ の元 α^i は冪指数 q 未満の元の線形和に変換できるため，最終的な出力は最大次数 $q-1$ の多項式表現，つまり長さ q のベクトル表現で乗算結果を出力する．

練習問題(5分)：乗算を計算してみよう

$GF(2^5)$ 上での $\alpha^3 \cdot \alpha^5$ を以下それぞれのケースで計算してみよ.
※解は4次以下の α の多項式で表現すること.

- $GF(2^5)$ が $p_1(x) = 1 + x^2 + x^5$ で定義されるケース
- $GF(2^5)$ が $p_2(x) = 1 + x + x^2 + x^4 + x^5$ で定義されるケース

乗算は複雑

拡大体を定義する既約多項式によって複雑度が変化する
$p_1(x)$ と $p_2(x)$ はどちらが大変だった？

項数が少ない既約多項式ほど乗算の複雑度が低い

拡大体を定義する既約多項式によって複雑度が変化する
$p_1(x)$ と $p_2(x)$ だと，$p_1(x)$ の方が計算が簡単.
既約多項式の項数が少ないほど，乗算の複雑度が低くなる

回路実装する際には拡大体を構成するための既約多項式として，できるだけ項数が少なくなる式を選択することが多い.

展開した乗算計算式: $p_2(x)$のほうが項数が多い

- $p_1(x)$のケース:

$$
\begin{aligned}
c_0 &= a_0b_0 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_4b_4 \\
c_1 &= a_0b_1 + a_1b_0 + a_2b_4 + a_3b_3 + a_4b_2 \\
c_2 &= a_0b_2 + a_1b_1 + a_1b_4 + a_2b_0 + a_2b_3 + a_3b_2 + a_3b_4 + a_4b_1 + a_4b_3 + a_4b_4 \\
c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_2b_4 + a_3b_0 + a_3b_3 + a_4b_2 + a_4b_4 \\
c_4 &= a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_3b_4 + a_4b_0 + a_4b_3
\end{aligned}
$$

- $p_2(x)$のケース

$$
\begin{aligned}
c_0 &= a_0b_0 + a_1b_4 + a_2b_3 + a_2b_4 + a_3b_2 + a_3b_3 + a_3b_4 + a_4b_1 + a_4b_2 + a_4b_3 \\
c_1 &= a_0b_1 + a_1b_0 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_4b_4 \\
c_2 &= a_0b_2 + a_1b_1 + a_1b_4 + a_2b_0 + a_2b_3 + a_3b_2 + a_3b_4 + a_4b_1 + a_4b_3 \\
c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_2b_4 + a_3b_0 + a_3b_3 + a_4b_2 + a_4b_4 \\
c_4 &= a_0b_4 + a_1b_3 + a_1b_4 + a_2b_2 + a_2b_3 + a_2b_4 + a_3b_1 + a_3b_2 + a_3b_3 + a_4b_0 + a_4b_1 + a_4b_2
\end{aligned}
$$

乗算器の回路実装について

- $p_1(x)$のケース:

$$
\begin{aligned}
c_0 &= a_0b_0 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_4b_4 \\
c_1 &= a_0b_1 + a_1b_0 + a_2b_4 + a_3b_3 + a_4b_2 \\
c_2 &= a_0b_2 + a_1b_1 + a_1b_4 + a_2b_0 + a_2b_3 + a_3b_2 + a_3b_4 + a_4b_1 + a_4b_3 + a_4b_4 \\
c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_2b_4 + a_3b_0 + a_3b_3 + a_4b_2 + a_4b_4 \\
c_4 &= a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_3b_4 + a_4b_0 + a_4b_3
\end{aligned}
$$

上式をそのまま回路実装する.
a_ib_j のANDゲートを q^2 個用意し，各ビット出力に必要なXORゲートを接続する.
演算器のオーダーは $O(q^3)$ となり，ガロア体演算器の中では逆元器の次に大きい.

ガロア体上でだいたいの線形代数が使える

- ガロア体上の n 次元空間 $GF(2^q)^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in GF(2^q)\}$
- 任意の部分空間 $V \subseteq GF(2^q)^n$ は加算とスカラー乗算において閉じている
  - $\forall \underline{v}, \underline{w} \in GF(2^q)^n, \forall \lambda \in GF(2^q), \underline{v} + \lambda \underline{w} \in GF(2^q)^n$
- $v_1, \ldots, v_t \in GF(2^q)^n$ が**線形独立**であるとは，すべての非零の要素 $\forall \lambda_1, \ldots, \lambda_n \in GF(2^q)$ において $\sum_i^t \lambda_i v_i \neq \underline{0}$
- 部分空間 $V \subseteq GF(2^q)^n$ の基底とは，V のすべての元を線形結合で表すことができる線形独立な $v_1, \ldots, v_t \in GF(2^q)^n$ の集合.
  - $V = \mathrm{span}(v_1, \ldots, v_t) = \{\sum_i^t \lambda_i v_i \mid \lambda_i \in GF(2^q)\}$
- 部分空間 $V \subseteq GF(2^q)^n$ の次元とは，V の基底 $\{v_1, \ldots, v_t\}$ のサイズ（元の数 t）.

※ ガロア体上の線形空間では，直交という概念はあるが，角度という概念はない.

ガロア体のまとめ

- 素体で素数を用いたように，既約多項式を用いることで，ガロア体 $GF(2^q)$を多項式の集合として定義できる.
- 原始元 α を持つ原始多項式でガロア体 $GF(2^q)$ を定義することが多い.
- ガロア体 $GF(2^q)$の元の表現
  - べき表現，多項式表現，ベクトル表現
  - べき表現は乗算に有利
  - ベクトル表現（多項式表現）は加算に有利
- 回路で実装する際にはベクトル表現を使うことが多い
- 乗算と既約多項式

演習

$p(x) = 1 + x^2 + x^3$ で定義された $GF(2^3)$ について，以下の問いに答えなさい．なお，(2)以降の計算は2次以下の α の多項式表現で答えること（α^3 のような答えは×）．

（1）スライド21に示したようなべき表現，多項式表現，ベクトル表現の表を作成せよ．スライド21とは$p(x)$が異なることに注意すること．
（2）$\alpha^3 + \alpha^4$ を計算せよ．
（3）$\alpha^3 \cdot \alpha^4$ を計算せよ．
（4）$\alpha^3 \div \alpha^4$ を計算せよ．